Friday, January 31, 2014

Beware the email foot-in-mouth syndrome

Daniel B. Garrie *is a partner at Law and Forensics.com, where he manages the E-Discovery, Forensics, and Computer Security practice Groups. Daniel splits his time between Seattle, Los Angeles and New York City. Daniel also serves as special counsel at Zeichner Ellman and Krause LLP. For more information, or with questions and comments, please email at Daniel@lawandforensics.com. Daniel would like to thank Kelsey Fredston-Hermann for her editorial assistance on this article. The views of Mr. Garrie are his own, and do not represent the views or opinions of Law and Forensics or Zeichner Ellman & Krause LLP.*

The modern world of corporate America runs on email and web-based applications. Consequently, the employees of corporate America are continuously sending emails, at all hours of the day and night, using their corporate email accounts. These emails, which must be automatically archived by the corporation in order to remain in compliance with data management regulations, frequently end up creating costly problems.

Here we discuss the relatively simple case of email "foot-in-mouth." Email communications can, and have, captured actually dishonest and illegal activities on the part of employees. Corporations must actively work to address and break the unthinking habits of employees armed with smartphones and mobile work email accounts.

One major problem with the ready availability and ubiquity of email and web-based applications is the information gap between top executives and mid- or lower-level employees. While IT security personnel may have educated upper-level executives on proper "email hygiene" and the permanence of email, other employees may be quite unaware of that aspect of their communications. The common-place assumption that emails can be permanently deleted by simply moving them to the trash folder is inaccurate, and can lead to serious trouble for an organization.

Take, for example, a case that emerged in the recent banking crisis: Mid-level Goldman Sachs trader Fabrice Tourre, known jokingly to his co-workers as "Fabulous Fab," sent several emails touting the role of the products he was selling in the looming banking catastrophe. "The whole building is about to collapse," he wrote, "anytime now ... Only potential survivor, the fabulous Fab ... standing in the middle of all these complex, highly leveraged, exotic trades he created without necessarily understanding all of the implications of those monstruosities [sic]!!!" *S.E.C. v. Goldman Sachs & Co., 790 F. Supp.* 2d 147, 150 (S.D.N.Y. 2011). This email, among others, arguably implicated Goldman Sachs with knowingly misleading investors. While the suit eventually resolved with Tourre being found liable for fraud, Goldman Sachs suffered from a loss of reputation, and had to endure a great deal of media outrage. His own ethics and business practices aside, Tourre clearly did not understand that anything written via a company email client, to paraphrase the Miranda warning, can and will be used against its author and the author's employer as well.

Another example involved the London Interbank Offered Rate, or "LIBOR," which is a key interest rate - an estimation of the rate that major London banks would pay if borrowing money from other banks - that affects borrowers throughout the world. In December 2012, amidst the infamous LIBOR-rigging scandal, the U.K.'s Financial Services Authority's report quoted UBS employee-emails in which those employees were attempting to control or manipulate the LIBOR rate. For example: "If you keep 6s

unchanged today ... I will f-- do one humongous deal with you ... Like a 50,000 buck deal, whatever ... I need you to keep it as low as possible ... if you do that ... I'll pay you, you know, 50,000 dollars, 100,000 dollars ... whatever you want ... I'm a man of my word." See Nick Summers, "The UBS Libor-Fraud Emails Are a Gift for Regulators," Dec. 19, 2012, Bloomberg Businessweek.

There are very few cases in which it is impossible for any of this data to be forensically retrieved or restored.

Despite the many high-profile cases involving email evidence, employees in corporate America still do not treat email, or the longevity of digital communications and documentation, with the respect it deserves. Employees and employers alike must remember that whatever the actual motivation or intent of the email or digital communication at issue, a badly worded employee email may wind up implicating the employee (and, by association, the company) in public scandal, with hundreds of millions of dollars on the line. Such emails can severely damage a company's business and reputation. In some cases, as for example with the now-defunct Arthur Anderson, the loss of reputation can in itself be a killing blow. When it comes to modern court cases, email and other digital evidence often comprises the difference between a winning and losing lawsuit.

For every email sent, there's an excellent chance is that someone, or many persons, may have kept a copy: the individual (both the sender and the receiver or receivers), the company mail server, the backup provider for either the sender or receiver, or the smart phone from which the email was sent. Regulations require that companies archive emails to some extent, and companies who practice in areas of greater government scrutiny and control (e.g., the healthcare or financial industries) are required by regulation to maintain and store vast amounts of data. There are very few cases in which it is impossible for any of this data to be forensically retrieved or restored. How, operating in a world where any unthinking (or improper) email sent by an employee could mean their employer's downfall, are companies to protect themselves?

I will leave the ethics education for companies to handle on their own. As for protecting against email folly, the solution is simple: use a tried and tested behavioral modification approach. Put a program in place that clearly outlines your company email policy (team this with a "bring your own device" policy for the greatest effect), and include examples of email communications that are prohibited during working hours, or from company email clients and via company machines. Let employees know that if they send an email violating any one of those policies, the company will take immediate action against them. This means that the next time an employee sends out, for benign example, a personal email about an eBay transaction while at work or via a work email account, the company will notify the user that such email communication is prohibited and notate the infraction on their employee file.

While this change in policy may be draconian, employees will adapt much faster than one might think, and it will alleviate the worries of countless legal counsels, IT security professionals, and indeed the employees themselves - this policy protects them as well, removing the risk of having their badly written or foolish personal communications from being meticulously and publicly examined in a court of law or in the media.

Daniel B. Garrie *is a partner at Law and Forensics.com, where he manages the E-Discovery, Forensics, and Computer Security practice Groups. Daniel splits his time between Seattle, Los Angeles and New York City. Daniel also serves as special counsel at Zeichner Ellman and Krause LLP. For more information, or with questions and comments, please email at Daniel@lawandforensics.com. Daniel would like to thank Kelsey Fredston-Hermann for her editorial assistance on this article. The views of Mr. Garrie are his own, and do not represent the views or opinions of Law and Forensics or Zeichner Ellman & Krause LLP.*